REMARKS

After entry of the foregoing amendment, claims 1-14 remain pending, unchanged.

Each of the claims stands rejected over McAuliffe (5,838,790) in view of Iwamura (6,425,081). Those rejections are respectfully traversed.

McAuliffe is understood to disclose an advertisement authentication system in which advertisements are downloaded for off-line display. The user's computer tracks which advertisements are presented to the user - and when (in an "advertisement statistics file" written on the user's hard disk), and the advertisers are billed accordingly. The McAuliffe system checks whether downloaded advertisements are modified or deleted, so that advertisers won't be billed for advertising that is not presented as intended to users.

More particularly, when McAuliffe transmits an advertisement to a user's computer, it additionally sends along an encrypted "fingerprint" of the advertisement, allowing the user's computer to determine whether any tampering occurred in the transmission process.[1]

When the user computer receives such an advertisement, it computes a fingerprint of the received advertisement, decrypts the encrypted fingerprint that was sent along with the advertisement, and compares the two for a match.[2] If the two don't match, a record is made in the advertisement statistics file, and the received advertisement is deleted.[3]

If the calculated and received/decrypted fingerprints match, McAuliffe stores the fingerprint in an encrypted file, and stores the authenticated advertisement in an advertisement directory on the user's hard disk.[4]

Thereafter, each time programming on the user's computer causes an advertisement to be displayed, it opens the encrypted file in which fingerprints are stored, and compares the stored fingerprint for the subject ad with a fingerprint newly computed from the ad.[5]

If the stored and calculated fingerprints do not match, McAuliffe does not proceed to display the ad, but instead stores an error message in the advertisement statistics file on

[1] McAuliffe, col. 3, lines 49-65; col. 4, lines 8-12; Fig. 1, box 106.

[2] McAuliffe, col. 7, lines 15-25.

[3] McAuliffe, col. 7, lines 15-33.

[4] McAuliffe, col. 7, lines 34-38.

[5] McAuliffe, col. 7, lines 48-53; col. 8, lines 7-17.

the user's hard disk noting the failed authentication.[6]

It will be recognized that – *contrary to the Examiner's statement in the Action* – McAuliffe does not check the integrity of fingerprint data. (Such an act is an express element of applicants' claim 1, and claims 2-7 dependent thereon.)

Instead, McAuliffe checks the correspondence between fingerprint data and an advertisement. The advertisement may be suspect. The fingerprint data is not. McAuliffe's system is based on fingerprints "*known to be secure*."[7]

Thus, if the stored and calculated fingerprint data don't match, this indicates corruption or alteration of the advertisement file.[8]

Another clause in applicants' claim 1 says "if the check leaves doubt about the fingerprint data..." Again, McAuliffe does not suggest any possible "doubt" about the fingerprint data.

Still further, applicants' claim 1 includes the act of "transmitting the fingerprint data to a database [if the check leaves doubt about the fingerprint data]." On this act, too, McAuliffe is silent. (The Examiner cites col. 8, lines 12-17 for such teaching, but this excerpt instead teaches storing an error message in the advertisement statistics file, and computing a fingerprint of the advertisement statistics file.)

Since the McAuliffe reference fails to teach that for which the Action cites it, a *prima facie* showing under Section 103 has not been established. Accordingly, applicants do not belabor this response by highlighting other shortcomings and errors in the Action, and its interpretation/application of the art.

The analysis of independent claim 8 – and claims dependent thereon - is similarly faulty. For example, claim 8 requires "checking the integrity of the watermark data." The Action again cites the excerpt at col. 8, lines 7-15 that deals with authenticating the advertisement, and terms it "checking the integrity of the data" (overlooking the "watermark" limitation in applicants' claims).

The Action then seeks to hybridize watermark teachings into McAuliffe's system, with the rationale:

[6] McAuliffe, col. 8, lines 11-15.

[7] McAuliffe, col. 3, line 58.

[8] McAuliffe, col. 7, lines 30-31; col. 8, lines 18-20.

> It would have been obvious to person of ordinary skill in the art at the time invention was made to use watermark data, as taught in Iwamura with data embedding method disclosed in McAuliffe because watermark data is preserved if the data is manipulated by processes such as compression or cropping.

As to this, it should first be noted that there is no "data embedding method disclosed in McAuliffe." On this point the Action is incorrect factually, and the rationale based thereon fails.

Moreover, concerning the purported rationale, it appears watermark's resilience to data manipulation makes it exactly what McAuliffe would avoid, rather than adopt. After all, McAuliffe's aim is to detect tampering. Since watermark data is preserved despite many forms of tampering, it appears McAuliffe's aim would be frustrated by adoption of such technology.

Again, the rejections fail to properly address other limitations of the claims, and are based on errors concerning the art and its purported application to the claims. However, since the points above are believed to demonstrate the lack of a *prima facie* case under Section 103, these other points aren't belabored.

Favorable reconsideration and passage to issuance are solicited.

Date: March 18, 2004

CUSTOMER NUMBER 23735

Phone: 503-885-9699
FAX 503-885-9880

Respectfully submitted,

DIGIMARC CORPORATION

By____________________
William Y. Conwell
Registration No. 31,943